BAB III
METODE PENELITIAN

Metode yang digunakan dalam penulisan skripsi adalah studi literatur dan pengembangan model, serta aplikasinya dalam program yang akan akan diuraikan secara rinci dalam langkah-langkah berikut:

3.1 Perumusan Masalah

Semakin berkembangnya teknologi informasi dan komunikasi dalam masyarakat, bukan hanya pengaksesan pesan saja yang berkembang pesat, pengaksesan citra digital pun meningkat. Citra digital merupakan data berbentuk digital seperti gambar dengan format yang berbeda-beda. Ketika pengaksesan gambar dilakukan, tidak jarang para peretas mengambil alih data yang akan dikirim atau diterima secara tidak bertanggungjawab. Sehingga pengirim harus mampu menjaga kerahasiaan gambar yang akan dikirim. Salah satu cara meningkatkan keamanannya dengan menggunakan kriptografi *Hill Cipher yaitu* penyandian gambar dengan kunci berupa matriks agar bentuknya teracak.

3.2 Model Dasar

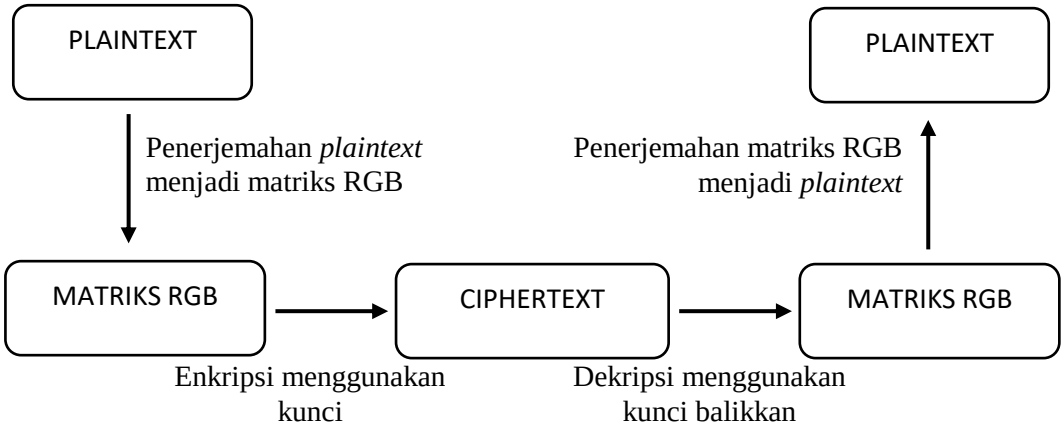
Algoritma *Hill Cipher* merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. *Hill Cipher* diciptakan oleh Lester S. Hill pada tahun 1929. Kriptografi ini diciptakan dengan tujuan mendapatkan *cipher* (kode) yang sulit untuk dipecahkan. *Hill Cipher* tidak mengganti setiap abjad yang sama pada plaintext dengan abjad lainnya yang sama pada ciphertext karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya.

Proses pengaplikasian algoritma *Hill Cipher* pada gambar hampir menyerupai penyandian yang dilakukan terhadap pesan teks. Hanya saja jika pada teks yang akan di enkripsi adalah abjadnya, sedangkan untuk gambar yang akan dieksekusi adalah kode-kode RGB pada setiap pixelnya. Kunci matriks yang

digunakan bisa ditentukan oleh pengirim dengan syarat matriks harus memiliki invers matriks dan invers modulo untuk proses dekripsinya.

3.3 Pengembangan Model Dasar

Pengembangan kriptografi *Hill Cipher* dalam skripsi ini adalah penggunaan algoritma *Hill Cipher* yang umumnya digunakan untuk meningkatkan keamanan pada pesan teks, akan digunakan pada citra digital berupa gambar. Sebelum proses enkripsi, gambar akan diterjemahkan kedalam matriks RGB. Selanjutnya barulah proses enkripsi dapat dilakukan dengan mengalikan matriks RGB dengan matriks kunci sehingga menghasilkan sebuah *ciphertext* yang siap untuk dikirim ke penerima. Untuk proses dekripsi, matriks kunci harus dibalik (invers) terlebih dahulu. Selanjutnya mengalikan *ciphertext* dengan kunci yang sudah dibalikkan untuk mendapatkan matriks RGB dan penerjemahan kembali matriks RGB untuk mendapatkan pesan gambar asli (*plaintext*).



Gambar 3. 1 *Rancangan Skema Penyandian Gambar*

3.4 Kontruksi Program Aplikasi

3.4.1 Perancangan Program Aplikasi

Pada tahap ini dilakukan perancangan tampilan untuk program enkripsi dan dekripsi seperti Tabel 3.1. Input dari program enkripsi adalah gambar *plaintext* dan matriks kunci dengan *output ciphertext*. Untuk proses dekripsi *input* dari programnya adalah *ciphertext* dan matriks kunci dengan *output plaintext.*

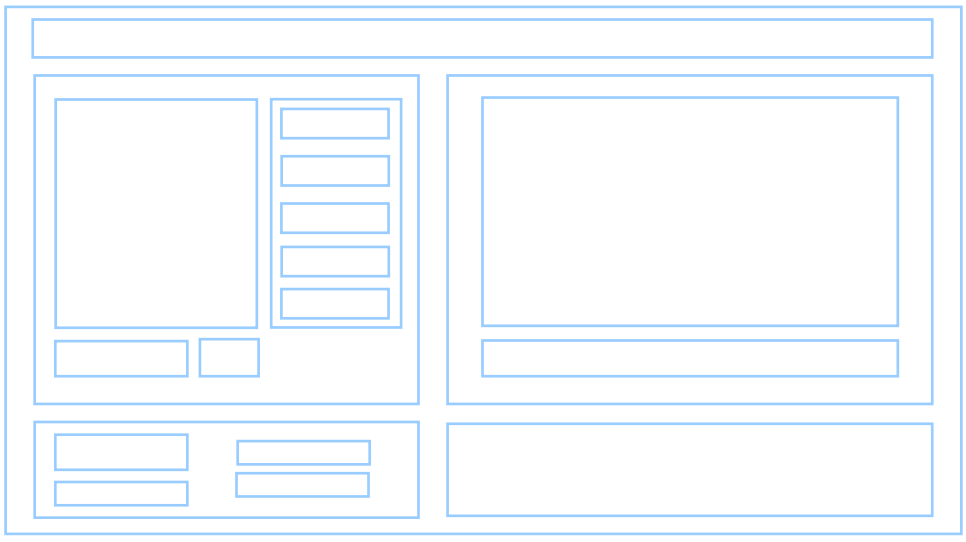
Tabel 3. 1 *Rancangan Program Enkripsi dan Dekripsi*

	Enkripsi	Dekripsi
Input	*Plaintext* Matriks Kunci	*Ciphertext* Matriks Kunci
Output	*Ciphertext*	*Plaintext*

3.4.2 Rancangan Tampilan Program Aplikasi

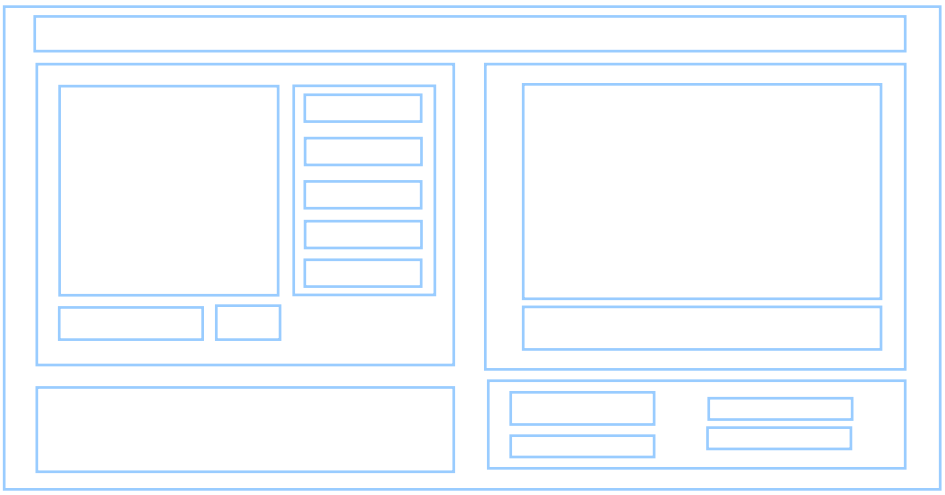
Implementasi kriptografi *Hill Cipher* pada penyandian gambar dibuat menggunakan aplikasi MATLAB GUI versi 9.0. Program tersebut bertujuan untuk memudahkan proses enkripsi dan dekripsi serta validasi pada penyandian gambar dengan menggunakan kriptografi *Hill Cipher*. Rancangan program aplikasi diberikan pada Tabel 3.2 berikut:

Tabel 3. 2 *Rancangan Tampilan Program Aplikasi*

Rancangan Tampilan
ENKRIPSI  **Keterangan:** - *Input* : *Plaintext* dan Kunci Matriks 2 x 2

- *Massage Box* : Ketersediaan Invers Matriks dan Invers Modulo 256
- *Output* : Informasi Gambar dan *Ciphertext*

DEKRIPSI



KETERANGAN:

- *Input : Ciphertext* dan Kunci Matriks 2 x 2
- *Output :* Informasi Gambar dan *Plaintext*

3.4.3 Algoritma Penyandian Gambar dengan menggunakan *Hill Cipher*

Proses enkripsi penyandian gambar menggunakan kriptografi *Hill Cipher* dapat dibagi ke beberapa tahap sebagai berikut:

1.4.3.1 Proses Enkripsi

1. Pengirim menentukan *plainteks* berupa gambar dengan format *.png dan berukuran m x n *pixel* genap. Ketika gambar diperbesar, maka akan terlihat blok-blok *pixel* seperti Gambar 3.2 berikut:

$Pixel_1$ $(r_{(1,1)}, g_{(1,1)}, b_{(1,1)})$	⋯	**$Pixel_n$** $(r_{(1,n)}, g_{(1,n)}, b_{(1,n)})$
⋮	⋱	⋮
$Pixel_m$ $(r_{(m,1)}, g_{(m,1)}, b_{(m,1)})$	⋯	**$Pixel_{m,n}$** $(r_{(m,n)}, g_{(m,n)}, b_{(m,n)})$

***Gambar 3. 2** Plaintext yang telah diperbesar*

2. Kemudian *Plaintext* diterjemahkan menjadi matriks *RGB*. Matriks *RGB* akan terbagi menjadi tiga bagian, yaitu matriks *Green* mewakili warna hijau, matriks *Red* mewakili warna merah, dan matriks *Blue* mewakili warna biru dari setiap *pixel* yang termuat di *plaintext.* Matriks *RGB* berikut:

$$R = \begin{bmatrix} r_{(1,1)} & \cdots & r_{(1,n)} \\ \vdots & \ddots & \vdots \\ r_{(m,1)} & \cdots & r_{(m,n)} \end{bmatrix}$$

$$G = \begin{bmatrix} g_{(1,m)} & \cdots & g_{(1,n)} \\ \vdots & \ddots & \vdots \\ g_{(m,1)} & \cdots & g_{(m,n)} \end{bmatrix}$$

$$B = \begin{bmatrix} b_{(1,1)} & \cdots & b_{(1,n)} \\ \vdots & \ddots & \vdots \\ b_{(m,1)} & \cdots & b_{(m,n)} \end{bmatrix}$$

Dengan m dan n adalah letak kolom dan baris dari kode warna tersebut.

3. Menentukan matriks kunci yang berordo 2 x 2. Sebelumnya harus dipastikan terlebih dahulu bahwa matriks tersebut memiliki invers modulo terhadap modulo 256. Kunci secara umum ditulis

$$K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

$$a, b, c, d \in \mathbb{Z}$$

Dengan invers matriks

$$K \,.\, K^{-1} = I$$

$$K^{-1} = \frac{1}{det} \,.\, Adj \;,\; det \neq 0$$

$$= \frac{1}{a.d - b.c} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

Karena proses penyandian terbatas pada modulo 256, maka determinan harus memiliki invers modulo sedemikian sehingga

$$= \left(\frac{1}{a.d - b.c} \; mod \; 256 \right) \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$= p\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$$= \begin{bmatrix} pd & p(-b) \\ p(-c) & pa \end{bmatrix}$$

$$= \begin{bmatrix} e & f \\ g & h \end{bmatrix}$$

dengan $p = \frac{1}{a.d-b.c} \ mod\ 256$;

$$e = pd;\ f = p(-b);\ g = p(-c);\ h = pa$$

4. Kemudian pengirim mengubah orde matriks *RGB* menjadi n x 2 agar dapat dikalikan dengan matriks kunci yang berordo 2 x 2, sedemikian sehingga

$$R = \begin{bmatrix} r_{(1,1)} & r_{(1,2)} \\ \vdots & \vdots \\ r_{(m,n-1)} & r_{(m,n)} \end{bmatrix}$$

$$G = \begin{bmatrix} g_{(1,1)} & g_{(1,2)} \\ \vdots & \vdots \\ g_{(m,n-1)} & g_{m,n} \end{bmatrix}$$

$$B = \begin{bmatrix} b_1 & b_2 \\ \vdots & \vdots \\ b_{(m,n-1)} & b_{m,n} \end{bmatrix}$$

5. Pada proses enkripsi, pengirim melakukan pengalian matriks *R*, *G*, dan *B* dengan matriks kunci. Selanjutnya dilakukan modulo 256 pada hasil perkalian tersebut. Berikut perhitungannya:

e(R) = R . K mod 256

$$= \begin{bmatrix} r_{(1,1)} & r_{(1,2)} \\ \vdots & \vdots \\ r_{(m,n-1)} & r_{(m,n)} \end{bmatrix} . \begin{bmatrix} a & b \\ c & d \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} r_{(1,1)} . a + r_{(1,2)} . c & r_{(1,1)} . b + r_{(1,2)} . d \\ \vdots & \vdots \\ r_{(m,n-1)} . a + r_{(m,n)} . c & r_{(m,n-1)} . b + r_{(m,n)} . d \end{bmatrix} mod\ 256$$

$$= \begin{bmatrix} x_{(1,1)} & x_{(1,2)} \\ \vdots & \vdots \\ x_{(m,n-1)} & x_{(m,n)} \end{bmatrix}$$

dengan

$$x_{(1,1)} = r_{(1,1)} . a + r_{(1,2)} . c$$

$$x_{(1,2)} = r_{(1,1)} . b + r_{(1,2)} . d$$
$$\vdots$$
$$x_{(m,n-1)} = r_{(m,n-1)} . a + r_{(m,n)} . c$$
$$x_{(m,n)} = r_{(m,n-1)} . b + r_{(m,n)} . d$$

e(G) = G . K mod 256

$$= \begin{bmatrix} g_{(1,1)} & g_{(1,2)} \\ \vdots & \vdots \\ g_{(m,n-1)} & g_{(m,n)} \end{bmatrix} . \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ mod } 256$$

$$= \begin{bmatrix} g_{(1,1)} . a + g_{(1,2)} . c & g_{(1,1)} . b + g_{(1,2)} . d \\ \vdots & \vdots \\ g_{(m,n-1)} . a + g_{(m,n)} . c & g_{(m,n-1)} . b + g_{(m,n)} . d \end{bmatrix} \text{ mod } 256$$

$$= \begin{bmatrix} y_{(1,1)} & y_{(1,2)} \\ \vdots & \vdots \\ y_{(m,n-1)} & y_{(m,n)} \end{bmatrix}$$

dengan

$$y_{(1,1)} = g_{(1,1)} . a + g_{(1,2)} . c$$
$$y_{(1,2)} = g_{(1,1)} . b + g_{(1,2)} . d$$
$$\vdots$$
$$y_{(m,n-1)} = r_{(m,n-1)} . a + r_{(m,n-1)} . c$$
$$y_{(m,n)} = r_{(m,n-1)} . b + r_{(m,n-1)} . d$$

e(B) = B . K mod 256

$$= \begin{bmatrix} b_{(1,1)} & b_{(1,2)} \\ \vdots & \vdots \\ b_{(m,n-1)} & b_{(m,n)} \end{bmatrix} . \begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ mod } 256$$

$$= \begin{bmatrix} b_{(1,1)} . a + b_{(1,2)} . c & b_{(1,1)} . b + b_{(1,2)} . d \\ \vdots & \vdots \\ b_{(m,n-1)} . a + b_{(m,n)} . c & b_{(m,n-1)} . b + b_{(m,n)} . d \end{bmatrix} \text{ mod } 256$$

$$= \begin{bmatrix} z_{(1,1)} & z_{(1,2)} \\ \vdots & \vdots \\ z_{(m,n-1)} & z_{(m,n-1)} \end{bmatrix}$$

dengan

$$z_{(1,1)} = b_{(1,1)} . a + b_{(1,2)} . c$$
$$z_{(1,2)} = b_{(1,1)} . b + b_{(1,2)} . d$$

$$\vdots$$

$$y_{(m,n-1)} = b_{(m,n-1)} \,.\, a + b_{(m,n)} \,.\, c$$

$$y_{(m,n)} = b_{(m,n-1)} \,.\, b + b_{(m,n)} \,.\, d$$

Sehingga diperoleh matriks

$$e(R) = \begin{bmatrix} x_{(1,1)} & x_{(1,2)} \\ \vdots & \vdots \\ x_{(m,n-1)} & x_{(m,n)} \end{bmatrix}$$

$$eG) = \begin{bmatrix} y_{(1,1)} & y_{(1,2)} \\ \vdots & \vdots \\ y_{(m,n-1)} & y_{(m,n)} \end{bmatrix}$$

$$e(B) = \begin{bmatrix} z_{(1,1)} & z_{(1,2)} \\ \vdots & \vdots \\ z_{(m,n-1)} & z_{(m,n)} \end{bmatrix}$$

6. Kemudian ubah kembali menjadi matriks *R*, *G*, dan *B* dengan ordo m x n seperti berikut:

$$R = \begin{bmatrix} x_{(1,1)} & \cdots & x_{(1,n)} \\ \vdots & \ddots & \vdots \\ x_{(m,1)} & \cdots & x_{(m,n)} \end{bmatrix}$$

$$G = \begin{bmatrix} y_{(1,m)} & \cdots & y_{(1,n)} \\ \vdots & \ddots & \vdots \\ y_{(m,1)} & \cdots & y_{(m,n)} \end{bmatrix}$$

$$B = \begin{bmatrix} z_{(1,1)} & \cdots & z_{(1,n)} \\ \vdots & \ddots & \vdots \\ z_{(m,1)} & \cdots & z_{(m,n)} \end{bmatrix}$$

7. *Ciphertext* adalah matriks *R*, *G*, dan *B* yang telah diterjemahkan kembali menjadi gambar seperti pada Gambar 3.3 berikut

Pixel$_1$ ($x_{(1,1)}$, $y_{(1,1)}$, $z_{(1,1)}$)	⋯	**Pixel$_n$** ($x_{(1,n)}$, $y_{(1,n)}$, $z_{(1,n)}$)
⋮	⋱	⋮
Pixel$_m$ ($x_{(m,1)}$, $y_{(m,1)}$, $z_{(m,1)}$)	⋯	**Pixel$_{m,n}$** ($x_{(m,n)}$, $y_{(m,n)}$, $z_{(m,n)}$)

Gambar 3. 3 *Ciphertext yang telah diperbesar*

8. *Ciphertext* yang dihasilkan adalah berupa gambar yang dengan format *.png. Pengirim kemudian mengirimkan *ciphertext* beserta kunci kepada penerima.

1.4.3.2 Proses Dekripsi

Proses dekripsi penyandian gambar dengan menggunakan kriptografi *Hill Cipher* dapat dibagi ke beberapa tahap sebagai berikut:

1. Penerima menerima *plaintext* dan kunci dari pengirim. Selanjutnya *ciphertext* diterjemahkan menjadi matriks *RGB* seperti pada tahap 3.1.1
2. Kemudian penerima mencari invers dari matriks kunci serta invers modulo dari matriks tersebut seperti langkah nomor 3 pada tahap 3.1.1.
3. Sebelum proses enkripsi, ubah orde matriks RGB menjadi n x 2. Selanjutnya penerima melakukan pengalian matriks *R*, *G*, dan *B* dengan invers matriks kunci. Selanjutnya dilakukan modulo 256 pada hasil perkalian tersebut. Berikut perhitungannya:

$$d(R) = R \,.\, K^{-1} \bmod 256$$

$$= \begin{bmatrix} x_{(1,1)} & x_{(1,2)} \\ \vdots & \vdots \\ x_{(m,n-1)} & x_{(m,n)} \end{bmatrix} . \begin{bmatrix} e & f \\ g & h \end{bmatrix} \bmod 256$$

$$= \begin{bmatrix} x_{(1,1)} \,.\, e + x_{(1,2)} \,.\, g & x_{(1,1)} \,.\, f + x_{(1,2)} \,.\, h \\ \vdots & \vdots \\ x_{(m,n-1)} \,.\, e + x_{(m,n)} \,.\, g & x_{(m,n-1)} \,.\, f + x_{(m,n)} \,.\, h \end{bmatrix} \bmod 256$$

$$= \begin{bmatrix} r_{(1,1)} & r_{(1,2)} \\ \vdots & \vdots \\ r_{(m,n-1)} & r_{(m,n)} \end{bmatrix}$$

dengan

$$\begin{aligned} r_{(1,1)} &= x_{(1,1)} \,.\, e + x_{(1,2)} \,.\, g \\ r_{(1,2)} &= x_{(1,1)} \,.\, f + x_{(1,2)} \,.\, h \\ &\vdots \\ r_{(m,n-1)} &= x_{(m,n-1)} \,.\, e + x_{(m,n)} \,.\, g \\ r_{(m,n)} &= x_{(m,n-1)} \,.\, f + x_{(m,n)} \,.\, h \end{aligned}$$

$$d(G) = G \,.\, K^{-1} \bmod 256$$

$$= \begin{bmatrix} y_{(1,1)} & y_{(1,2)} \\ \vdots & \vdots \\ y_{(m,n-1)} & y_{(m,n)} \end{bmatrix} . \begin{bmatrix} e & f \\ g & h \end{bmatrix} \text{ mod } 256$$

$$= \begin{bmatrix} y_{(1,1)} . e + y_{(1,2)} . g & y_{(1,1)} . f + y_{(1,2)} . h \\ \vdots & \vdots \\ y_{(m,n-1)} . e + y_{(m,n)} . g & y_{(m,n-1)} . f + y_{(m,n)} . h \end{bmatrix} \text{ mod } 256$$

$$= \begin{bmatrix} g_{(1,1)} & g_{(1,2)} \\ \vdots & \vdots \\ g_{(m,n-1)} & g_{(m,n)} \end{bmatrix}$$

dengan

$$g_{(1,1)} = y_{(1,1)} . e + y_{(1,2)} . g$$
$$g_{(1,2)} = y_{(1,1)} . f + y_{(1,2)} . h$$
$$\vdots$$
$$g_{(m,n-1)} = y_{(m,n-1)} . e + y_{(m,n)} . g$$
$$g_{(m,n)} = y_{(m,n-1)} . f + y_{(m,n)} . h$$

$d(B) = B \,.\, K^{-1} \text{ mod } 256$

$$= \begin{bmatrix} z_{(1,1)} & z_{(1,2)} \\ \vdots & \vdots \\ z_{(m,n-1)} & z_{(m,n)} \end{bmatrix} . \begin{bmatrix} e & f \\ g & h \end{bmatrix} \text{ mod } 256$$

$$= \begin{bmatrix} z_{(1,1)} . e + z_{(1,2)} . g & z_{(1,1)} . f + z_{(1,2)} . h \\ \vdots & \vdots \\ z_{(m,n-1)} . e + z_{(m,n)} . g & z_{(m,n-1)} . f + z_{(m,n)} . h \end{bmatrix} \text{ mod } 256$$

$$= \begin{bmatrix} b_{(1,1)} & b_{(1,2)} \\ \vdots & \vdots \\ b_{(m,n-1)} & b_{(m,n)} \end{bmatrix}$$

dengan

$$b_{(1,1)} = z_{(1,1)} . e + z_{(1,2)} . g$$
$$b_{(1,2)} = z_{(1,1)} . f + z_{(1,2)} . h$$
$$\vdots$$
$$b_{(m,n-1)} = z_{(m,n-1)} . e + z_{(m,n)} . g$$
$$b_{(m,n)} = z_{(m,n-1)} . f + z_{(m,n)} . h$$

Sehingga diperoleh matriks

$$e(R) = \begin{bmatrix} r_{(1,1)} & r_{(1,2)} \\ \vdots & \vdots \\ r_{(m,n-1)} & r_{(m,n)} \end{bmatrix}$$

$$e(G) = \begin{bmatrix} g_{(1,1)} & g_{(1,2)} \\ \vdots & \vdots \\ g_{(m,n-1)} & g_{(m,n)} \end{bmatrix}$$

$$e(B) = \begin{bmatrix} b_{(1,1)} & b_{(1,2)} \\ \vdots & \vdots \\ b_{(m,n-1)} & b_{(m,n)} \end{bmatrix}$$

4. Ubah kembali ordo matriks RGB menjadi n x m. Kemudian terjemahkan kembali menjadi gambar. Pada tahap ini, *ciphertext* akan berubah kembali menjadi *plaintext.*

3.1 Validasi

Pada tahap ini dilakukan validasi dari hasil output program yang telah dirancang. Hal ini dilakukan untuk mengetahui apakah terjemahan dari *plaintext* ke matriks RGB yang dienkripsi dengan kunci yang ditentukan dapat didekripsi hingga mengembalikannya menjadi *plaintext*.

3.2 Penarikan Kesimpulan

Tahap ini merupakan tahapan terakhir dari langkah-langkah penelitian, yaitu menarik kesimpulan dari hasil penelitian yang telah dilakukan sehingga dapat memberikan rekomendasi yang lebih baik untuk penelitian selanjutnya.